在 VMware 上部署 ASA Virtual

您可以在能够运行 VMware ESXi 的任何服务器类 x86 CPU 设备上部署 ASA Virtual。

重要事项 ASA Virtual的最低内存要求为2GB。如果当前 ASA Virtual的内存少于2GB，您将无法在不增加 ASA Virtual机内存的情况下，从早期版本升级到 9.13(1) 及更高版本。您也可以使用最新版本重新部署新的 ASA Virtual机。

准则和限制

您可以在 ESXi 服务器上创建和部署多个 ASA Virtual实例。根据所需部署的实例数量和使用要求，ASA Virtual部署所使用的具体硬件可能会有所不同。创建的每台虚拟设备都需要主机满足最低资源配置要求，包括内存、CPU 数量和磁盘空间。

重要事项 ASA Virtual部署时的磁盘存储大小为 8GB。无法更改磁盘空间的资源配置。

在部署 ASA Virtual之前，请查看以下准则和限制。

VMware ESXi 上的 ASA Virtual系统要求

请确保遵循以下规范，以确保最佳性能。ASA VirtualASA Virtual 具有以下要求：

- 主机 CPU 必须是包含虚拟化扩展的基于 x86 的服务器类 Intel 或 AMD CPU。

  例如，ASA Virtual性能测试实验室最少使用以下设备：使用以 2.6GHz 运行的 Intel® Xeon® CPU E5-2690v4 处理器的 Cisco Unified Computing System™ (Cisco UCS®) C 系列 M4 服务器。

- ASA Virtual 支持 ESXi 版本 6.0、6.5、6.7、7.0、7.0 升级 1、7.0 升级 2、7.0 升级 3和 8.0。有关不同 ASA Virtual 版本支持的 ESXi 版本的信息，请参阅 Cisco Secure Firewall ASA 兼容性。

建议的 vNIC

推荐使用以下 vNIC 以获得最佳性能。

- PCI 直通中的 i40e - 将服务器的物理 NIC 指定给 VM，并通过 DMA（直接内存访问）在 NIC 与 VM 之间传输数据包数据。移动数据包不需要任何 CPU 周期。
- i40evf/ixgbe-vf - 基本同上（在 NIC 与 VM 之间传输 DMA 数据包），但允许在多个 VM 之间共享 NIC。SR-IOV 通常是首选的，因为它具有更多部署灵活性。请参阅准则和限制，第 27 页
- vmxnet3 - 这是并行虚拟化的网络驱动程序，支持 10Gbps 操作，但也需要 CPU 周期。这是 VMware 默认设置。

  如果使用 vmxnet3，则需要禁用 Large Receive Offload (LRO)，以免 TCP 性能不佳。

性能优化

为实现 ASA Virtual的最佳性能，您可以对 VM 和主机进行调整。有关详细信息，请参阅 性能调优，第 22 页。

- **NUMA** - 您可以通过将来宾 VM 的 CPU 资源隔离到单一非一致内存访问 (NUMA) 节点来提高 ASA Virtual的性能。有关详细信息，请参阅 NUMA 准则，第 22 页。
- **接收端扩展** - ASA Virtual 支持接收端扩展 (RSS)，网络适配器利用这项技术将网络接收流量分发给多个处理器内核。受 9.13 (1) 和更高版本的支持。有关详细信息，请参阅用于接收端扩展 (RSS) 的多个 RX 队列，第 24 页。
- **VPN 优化 (VPN Optimization)** - 有关使用 ASA Virtual优化 VPN 性能的其他注意事项，请参阅 VPN 优化。

集群

从版本 9.17 开始，VMware 上部署的 ASA Virtual 实例支持集群。有关详细信息，请参阅 ASAv 的 ASA 集群。

OVF 文件准则

选择 asav-vi.ovf 还是 asav-esxi.ovf 文件取决于部署目标：

- Asav-vi - 适用于部署在 vCenter 上

- Asav-esxi - 适用于部署在 ESXi 上（无 vCenter）
- ASA Virtual OVF 部署不支持本地化（在非英语模式下安装组件）。请确保在 ASCII 兼容模式下在您的环境中安装 VMware vCenter 和 LDAP 服务器。
- 在安装 ASA Virtual 之前，必须将键盘设置成美国英语，才能使用 VM 控制台。
- 部署 ASA Virtual时，ESXi 虚拟机监控程序上将安装两个不同的 ISO 映像：
  - 安装的第一个驱动器具有 vSphere 生成的 OVF 环境变量。
  - 安装的第二个驱动器是 day0.iso。

注意 ASA Virtual机启动后，您可以卸下这两个驱动器。但是，即使未选中**启动时连接 (Connect at Power On)**，每次 ASA Virtual断电/通电时，也总是会安装驱动器 1（带 OVF 环境变量）。

导出 OVF 模板准则

vSphere 中的导出 OVF 模板可帮助您将现有 ASA Virtual实例包导出为 OVF 模板。您可以使用导出的 OVF 模板在相同或不同的环境中部署 ASA Virtual 实例。在 vSphere 上使用导出的 OVF 模板部署 ASA Virtual实例之前，必须修改 OVF 文件中的配置详细信息，以防止部署失败。

修改导出的 ASA Virtual OVF 文件。

1. 登录到已导出 OVF 模板的本地计算机。
2. 浏览并在文本编辑器中打开 OVF 文件。
3. 确保存在标签 `<vmw:ExtraConfig vmw:key="monitor_control.pseudo_perfctr" vmw:value="TRUE"></vmw:ExtraConfig>`。
4. 删除标签 `<rasd:ResourceSubType>vmware.cdrom.iso</rasd:ResourceSubType>`。

   或

   替换标签 `<rasd:ResourceSubType>vmware.cdrom.iso</rasd:ResourceSubType>` with `<rasd:ResourceSubType>vmware.cdrom.remotepassthrough</rasd:ResourceSubType>`。

   有关详细信息，请参阅 VMware 发布的在 vCenter Server 5.1/5.5 上部署 OVF 失败 (2034422)。
5. 输入 `UserPrivilege`、`OvfDeployment` 和 `ControllerType` 的属性值。

   例如：

```
- <Property ovf:qualifiers="ValueMap{"ovf", "ignore", "installer"}" ovf:type="string"
ovf:key="OvfDeployment">
+ <Property ovf:qualifiers="ValueMap{"ovf", "ignore", "installer"}" ovf:type="string"
ovf:key="OvfDeployment" ovf:value="ovf">

- <Property ovf:type="string" ovf:key="ControllerType">
+ <Property ovf:type="string" ovf:key="ControllerType" ovf:value="ASAv">

- <Property ovf:qualifiers="MinValue(0) MaxValue(255)" ovf:type="uint8"
ovf:key="UserPrivilege">
```

```
+ <Property ovf:qualifiers="MinValue(0) MaxValue(255)" ovf:type="uint8"
ovf:key="UserPrivilege" ovf:value="15">
```

6. 保存 OVF 文件。
7. 使用 OVF 模板来部署 ASA Virtual。请参阅使用 VMware vSphere Web 客户端部署 ASA Virtual。

通过故障转移实现高可用性准则

对于故障转移部署，请确保备用设备具有相同的许可证权利；例如，两台设备均应具备 2Gbps 权限。

重要事项 使用 ASA Virtual创建高可用性对时，需要按相同顺序将数据接口添加到每个 ASA Virtual。如果完全相同的接口添加到每个 ASA Virtual，但采用不同的顺序，在 ASA Virtual控制台上会显示错误。故障转移功能可能也会受到影响。

对于用于 ASA Virtual 内部接口或 ASA Virtual 故障转移高可用性链路的 ESX 端口组，请配置两个虚拟 NIC 的 ESX 端口组故障转移顺序 - 一个作为活动上行链路，另一个作为备用上行链路。这是两个虚拟机相互 ping 或建立 ASA Virtual 高可用性链路所必需的。

IPv6 准则

首次使用 VMware vSphere Web 客户端部署 ASA Virtual OVF 文件时，不能为管理接口指定 IPv6 地址；您可以在以后使用 ASDM 或 CLI 添加 IPv6 地址。

使用 vMotion 的原则

- 按照 VMware 的要求，如果您计划使用 vMotion，则只能使用共享存储。部署 ASA Virtual 期间，如果有主机集群，则可以在本地（特定主机上）或在共享主机上调配存储。但是，如果您尝试使用 vMotion 将 ASA Virtual 移至其他主机，使用本地存储会造成错误。

适合吞吐量和许可的内存和 vCPU 分配

- 分配给 ASA Virtual 的内存大小专门针对吞吐量级别而定。除非您为不同的吞吐量级别申请许可证，否则不要在编辑设置对话框中更改内存设置或任何 vCPU 硬件设置。配置不足可能会影响性能。

注释 如果需要更改内存或 vCPU 硬件设置，请仅使用许可 ASA Virtual中记录的值。不要使用 VMware 建议的内存配置最小值、默认值和最大值。

CPU 预留

- 默认情况下，ASA Virtual预留的 CPU 大小为 1000 MHz。您可以使用共享、预留和限制设置（编辑设置 > 资源 > CPU）更改分配给 ASA Virtual的 CPU 资源量。如果 ASA Virtual可以较低的设

置在要求的流量负载下执行其所需的任务，则可以从 1000 MHz 降低 CPU 预留设置。ASA Virtual 使用的 CPU 大小取决于正在运行的硬件平台以及正在进行的工作的类型和数量。

对于所有虚拟机，您可以从 CPU 使用率 (Mhz) 图（位于虚拟机性能选项卡的主页视图中）中查看主机的 CPU 使用率信息。建立 ASA Virtual处理典型流量时的 CPU 使用率基准后，您可以依据该信息来调整 CPU 预留设置。

有关详细信息，请参阅 VMware 发布的 CPU 性能增强建议。

- 您可以使用 ASA Virtual **show vm** 和 **show cpu** 命令或者 ASDM **主页 (Home)** > **设备控制面板 (Device Dashboard)** > **设备信息 (Device Information)** > **虚拟资源 (Virtual Resources)** 选项卡或者 **健康 (Monitoring)** > **属性 (Properties)** > **系统资源图 (System Resources Graphs)** > **CPU** 窗格来查看资源配置以及任何过度调配或调配不足的资源。
- 从 ASA Virtual 版本 9.16.x 开始，当您从设备配置为 16 vCPU 和 32GB RAM 的 ASAv100 降级到 ASAv10 时，您必须为设备配置 1 vCPU 和 4GB RAM。

在 UCS B 系列硬件中使用透明模式的原则

据报告，一些配置为在思科 UCS B 系列硬件中以透明模式运行的 ASA Virtual存在 MAC 漂移问题。如果 MAC 地址显示为来自不同位置，则会造成丢包。

在 VMware 环境中以透明模式部署 ASA Virtual时，遵循下述原则可帮助您预防 MAC 漂移问题：

- VMware NIC 组合 - 如需在 UCS B 系列硬件上以透明模式部署 ASA Virtual，用于内部和外部接口的端口组必须只能有 1 个完全相同的活动上行链路。VMware NIC 组合可在 vCenter 中进行配置。

  有关如何配置 NIC 组合的完整信息，请参阅 VMware 文档。

- ARP 检测 - 在 ASA Virtual上启用 ARP 检测，然后在预期的接收接口上静态配置 MAC 和 ARP 条目。有关 ARP 检测功能及如何激活此功能的详细信息，请参阅《Cisco Secure Firewall ASA 系列通用操作配置指南》。

其他准则和限制

- 如果您运行的是 ESXi 6.7、vCenter 6.7、ASA Virtual 9.12 及更高版本，ASA Virtual 将在没有两个 CD/DVD IDE 驱动器的情况下启动。
- ASA Virtual OVF 部署不支持 vSphere Web 客户端；请改用 vSphere 客户端。

使用矢量数据包处理的 IPsec 流分流

您可以识别并选择要分流到超快路径的流量，其中流在 NIC 本身中进行切换。分流可帮助您提高数据密集型应用（例如大型文件传输）的性能。在初始设置 IPsec 站点到站点 VPN 或远程访问 VPN 安全关联 (SA) 后，IPsec 连接可卸载到 ASA Virtual 设备中的矢量包处理 (VPP)。

注释 IPsec 数据流分流已默认启用，并适用于设备 - ASAv100。

VPP 是思科开发的一款开源应用程序，用于 IPsec 分流，以执行 IPsec 加密操作。

在 ASA Virtual 上启用 IPsec 分流功能有助于：

- 提高设备性能并释放 CPU 资源以处理其他重要任务。
- 提高 IPsec 连接的总吞吐量性能。
- 提高 IPsec 的单连接性能，也称为大象流。

在支持此功能的平台上会默认禁用此功能。

限制

不分流以下 IPsec 流：

- IKEv1 隧道。在 ASAv100 上启用后，仅 IKEv2、ESP 和 NAT-T 会自动分流。IKEv2 支持更强的密码。
- 已配置压缩的流。
- 已配置压缩的流。
- 传输模式流。仅会分流隧道模式流。
- 已配置后分段的流。
- 防重放窗口大小不是 64 位且防重放的流不会被禁用。
- 防重放窗口大小不是 64 位且防重放的流不会被禁用。
- 已启用防火墙过滤器的流。
- 多情景

有关在 VMware vSphere Web 客户端上部署期间启用 IPsec 分流的信息，请参阅使用 VMware vSphere Web 客户端部署 ASA Virtual，第 12 页。

ASA Virtual的 VMware 功能支持

下表列出了 ASA Virtual的 VMware 功能支持。

表 *1: ASA Virtual*的 *VMware* 功能支持

功能	说明	支持（是/否）	备注
冷克隆	VM 在克隆过程中关闭。	是	–
DRS	用于动态资源调度和分布式电源管理。	是	不符合条件。

功能	说明	支持（是/否）	备注
热添加	VM 在添加过程中运行。	否	–
热克隆	VM 在克隆过程中运行。	否	–
热删除	VM 在删除过程中运行。	否	–
快照	VM 会冻结几秒钟。	是	请谨慎使用。您可能会失去流量。可能出现故障转移。
暂停和恢复	VM 暂停，然后恢复。	是	–
vCloud Director	允许自动部署 VM。	否	–
VM 迁移	VM 在迁移过程中关闭。	是	–
vMotion	用于实时迁移 VM。	是	使用共享存储。请参阅使用 vMotion 的原则，第 4 页。
VMware FT	用于 VM 上的 HA。	否	对 ASA Virtual机故障使用 ASA Virtual 故障转移。
VMware HA	用于 ESXi 和服务器故障。	是	对 ASA Virtual机故障使用 ASA Virtual 故障转移。
带 VM 心跳信号的 VMware HA	用于 VM 故障。	否	对 ASA Virtual机故障使用 ASA Virtual 故障转移。
VMware vSphere 独立 Windows 客户端	用于部署 VM。	是	–
VMware vSphere Web 客户端	用于部署 VM。	是	–

前提条件

您可以使用 VMware vSphere Web 客户端、vSphere 独立客户端或 OVF 工具部署 ASA Virtual。有关系统要求，请参阅思科 Cisco Secure Firewall ASA 兼容性。

vSphere 标准交换机的安全策略

对于 vSphere 交换机，您可以编辑第 2 层安全策略，并对 ASA Virtual 接口使用的端口组应用安全策略例外。请参阅以下默认设置：

- 混合模式：**拒绝**
- MAC 地址更改：**接受**
- 伪传输：**接受**

您可能需要为后面的 ASA Virtual配置修改这些设置。有关详细信息，请参阅 vSphere 文档。

表 *2:* 端口组安全策略例外

	路由防火墙模式		透明防火墙模式	
安全例外	无故障转移	故障转移	无故障转移	故障转移
混合模式	<任意>	<任意>	接受	接受
MAC 地址更改	<任意>	接受	<任意>	接受
伪传输	<任意>	接受	接受	接受

解压缩 ASA Virtual软件并创建 Day 0 配置文件

在启动 ASA Virtual之前，您可以准备一个 Day 0 配置文件。此文件是包含将在 ASA Virtual 启动时应用的 ASA Virtual 配置的文本文件。此初始配置将放入您选择的工作目录中名为“day0-config”的文本文件，并写入首次启动时安装和读取的 day0.iso 文件。Day 0 配置文件必须至少包含用于激活管理接口以及设置用于公共密钥身份验证的 SSH 服务器的命令，但它还可包含完整的 ASA 配置。该版本附带一个包含空 day0-config 的默认 day0.iso。day0.iso 文件（自定义 day0.iso 或默认 day0.iso）必须在首次启动过程中可用。

开始之前

我们在本示例中使用的是 Linux，但对于 Windows 也有类似的实用程序。

- 要在初始部署过程中自动完成 ASA Virtual 的许可过程，请将从思科智能软件管理器下载的智能许可身份 (ID) 令牌放入与 Day 0 配置文件处于同一目录且名为“idtoken”的文本文件。

- 如果需要从虚拟机监控程序的**串行端口**（而不是虚拟 VGA 控制台）访问和配置 ASA Virtual，则 Day 0 配置文件中应包括 console serial 设置，才能在首次启动过程中使用串行端口。
- 如果要在透明模式下部署 ASA Virtual，则必须在透明模式下将已知的运行 ASA 配置文件用作 Day 0 配置文件。这不适用于路由防火墙的 Day 0 配置文件。
- 有关如何在 ESXi 虚拟机监控程序上安装 ISO 映像的其他信息，请参阅 准则和限制，第 1 页中的 OVF 文件准则。

过程

步骤 1 从 Cisco.com 下载压缩文件，并将其保存到本地磁盘：

https://www.cisco.com/go/asa-software

注释
需要 Cisco.com 登录信息和思科服务合同。

步骤 2 将该文件解压缩到工作目录。请勿删除该目录中的任何文件。其中包括以下文件：

- asav-vi.ovf - 适用于 vCenter 部署。
- asav-esxi.ovf - 适用于非 vCenter 部署。
- boot.vmdk - 启动磁盘映像。
- disk0.vmdk - ASA Virtual磁盘映像。
- day0.iso - 包含 day0-config 文件和 idtoken 文件（可选）的 ISO。
- asav-vi.mf - 适用于 vCenter 部署的清单文件。
- asav-esxi.mf - 适用于非 vCenter 部署的清单文件。

步骤 3 在名为“day0-config”的文本文件中输入 ASA Virtual的 CLI 配置。添加三个接口的接口配置和所需的任何其他配置。

第一行应以 ASA 版本开头。day0-config 应该是有效的 ASA 配置。生成 day0-config 的最佳方式是从现有的 ASA 或 ASA Virtual复制一个运行配置的所需部分。day0-config 中的行顺序很重要，应与现有的 **show running-config** 命令输出中看到的顺序相符。

我们提供了两个 day0-config 文件的示例。第一个示例显示部署带千兆位以太网接口的 ASA Virtual时的 day0-config。第二个示例显示部署带万兆位以太网接口的 ASA Virtual时的 day0-config。您可以使用此 day0-config 来部署带 SR-IOV 接口的 ASA Virtual；请参阅准则和限制，第 27 页。

示例：

```
ASA Version 9.4.1
!
console serial
interface management0/0
nameif management
security-level 100
```

```
ip address 192.168.1.1 255.255.255.0
no shutdown
interface gigabitethernet0/0
nameif inside
security-level 100
ip address 10.1.1.2 255.255.255.0
no shutdown
interface gigabitethernet0/1
nameif outside
security-level 0
ip address 198.51.100.2 255.255.255.0
no shutdown
http server enable
http 192.168.1.0 255.255.255.0 management
crypto key generate rsa modulus 1024
username AdminUser password paSSw0rd
ssh 192.168.1.0 255.255.255.0 management
aaa authentication ssh console LOCAL
call-home
http-proxy 10.1.1.1 port 443
license smart
feature tier standard
throughput level 2G
```

示例：

```
ASA Version 9.8.1
!
console serial
interface management 0/0
management-only
nameif management
security-level 0
ip address 192.168.0.230 255.255.255.0
!
interface GigabitEthernet0/0
nameif inside
security-level 100
ip address 10.10.10.10 255.255.255.0
ipv6 address 2001:10::1/64
!
interface GigabitEthernet0/1
nameif outside
security-level 0
ip address 10.10.20.10 255.255.255.0
ipv6 address 2001:20::1/64
!
route management 0.0.0.0 0.0.0.0 192.168.0.254
!
username cisco password cisco123 privilege 15
!
aaa authentication ssh console LOCAL
ssh 0.0.0.0 0.0.0.0 management
ssh timeout 60
ssh version 2
!
http 0.0.0.0 0.0.0.0 management
!
logging enable
logging timestamp
logging buffer-size 99999
logging buffered debugging
logging trap debugging
!
dns domain-lookup management
```

```
DNS server-group DefaultDNS
name-server 64.102.6.247
!
license smart
feature tier standard
throughput level 10G
!
crypto key generate rsa modulus 2048
```

步骤 4 （可选）将思科智能软件管理器发布的智能许可证身份令牌文件下载到您的 PC。

步骤 5 （可选）从下载文件复制 ID 令牌并将其放入仅包含 ID 令牌的名为“idtoken”的文本文件。

身份令牌自动向智能许可服务器注册 ASA Virtual。

步骤 6 通过将文本文件转换成 ISO 文件生成虚拟 CD-ROM：

示例：

```
stack@user-ubuntu:-/KvmAsa$ sudo genisoimage -r -o day0.iso day0-config idtoken
I: input-charset not specified, using utf-8 (detected in locale settings)
Total translation table size: 0
Total rockridge attributes bytes: 252
Total directory bytes: 0
Path table size (byptes): 10
Max brk space used 0
176 extents written (0 MB)
stack@user-ubuntu:-/KvmAsa$
```

步骤 7 在 Linux 上计算 day0.iso 的新 SHA1 值：

示例：

```
openssl dgst -sha1 day0.iso
SHA1(day0.iso)= e5bee36e1eb1a2b109311c59e2f1ec9f731ecb66 day0.iso
```

步骤 8 在工作目录的 asav-vi.mf 文件中包括新的校验和，并将 day0.iso SHA1 值替换为新生成的值。

示例：

```
SHA1(asav-vi.ovf)= de0f1878b8f1260e379ef853db4e790c8e92f2b2
SHA1(disk0.vmdk)= 898b26891cc68fa0c94ebd91532fc450da418b02
SHA1(boot.vmdk)= 6b0000ddebfc38ccc99ac2d4d5dbfb8abfb3d9c4
SHA1(day0.iso)= e5bee36e1eb1a2b109311c59e2f1ec9f731ecb66
```

步骤 9 将 day0.iso 文件复制到您将压缩文件解压缩到的位置。您将覆盖默认的空 day0.iso 文件。

在从该目录复制任何虚拟机时，系统会应用新生成的 day0.iso 内的配置。

使用 VMware vSphere Web 客户端部署 ASA Virtual

本节介绍如何使用 VMware vSphere Web 客户端部署 ASA Virtual。Web 客户端需要 vCenter。如果您没有 vCenter，请参阅使用 VMware vSphere 独立客户端和 Day 0 配置来部署 ASA Virtual，或使用 OVF 工具和 Day 0 配置来部署 ASA Virtual。

- 访问 vSphere Web 客户端并安装客户端集成插件 ， 第 12 页

• 使用 VMware vSphere Web 客户端部署 ASA Virtual，第 11 页

访问 vSphere Web 客户端并安装客户端集成插件

本节介绍如何访问 vSphere Web 客户端。本节还介绍如何安装客户端集成插件，该插件是访问 ASA Virtual控制台所必需的。Macintosh 不支持某些 Web 客户端功能（包括插件）。请参阅 VMware 网站获取完整的客户端支持信息。

过程

步骤 1 从浏览器启动 VMware vSphere Web 客户端：

https://*vCenter_server:port***/vsphere-client/**

默认情况下，端口为 9443。

步骤 2 （仅需一次）安装客户端集成插件，以便访问 ASA Virtual控制台。

1. 在登录屏幕中，点击**下载客户端集成插件 (Download the Client Integration Plug-in)** 以下载插件。
2. 关闭浏览器，然后使用安装程序安装插件。
3. 安装插件后，重新连接到 vSphere Web 客户端。

步骤 3 输入用户名和密码，然后点击**登录 (Login)**，或选中**使用 Windows 会话身份验证 (使用 Windows 会话身份验证)** 复选框（仅限 Windows）。

使用 VMware vSphere Web 客户端部署 ASA Virtual

要部署 ASA Virtual，请使用 VMware vSphere Web 客户端（或 vSphere 客户端）和开放式虚拟化格式 (OVF) 的模板文件。在 vSphere Web 客户端中使用 Deploy OVF Template 向导来部署 ASA Virtual 的思科软件包。该向导将解析 ASA Virtual OVF 文件，创建将运行 ASA Virtual 的虚拟机，并安装软件包。

大多数向导步骤是 VMware 的标准步骤。有关部署 OVF 模板的更多信息，请参阅 VMware vSphere Web 客户端联机帮助。

开始之前

在部署 ASA Virtual 之前，您必须在 vSphere 中配置至少一个网络（用于管理）。

过程

步骤 1 从 Cisco.com 下载 ASA Virtual 压缩文件，并将其保存到 PC：

http://www.cisco.com/go/asa-software

注释
需要 Cisco.com 登录信息和思科服务合同。

步骤 2 在 vSphere Web 客户端的**导航器 (Navigator)** 窗格中，点击 **vCenter**。

步骤 3 点击**主机和集群 (Hosts and Clusters)**。

步骤 4 右键点击要部署 ASA Virtual 的数据中心、集群或主机，然后选择**部署 OVF 模板 (Deploy OVF Template)**。此时将出现“**部署 OVF 模板**”**(Deploy OVF Template)** 向导。

步骤 5 按照向导屏幕的指示操作。

从 Cisco Secure Firewall ASA 版本 9.22 的 **配置** 窗口中，您可以选择 **ASAvU - 32 核/64 GB** 或 **ASAvU - 64 核/128 GB** 部署配置，以删除速率限制器。有关 ASAvU 许可证的详细信息，请参阅 ASA Virtual 的许可。

步骤 6 在**设置网络**屏幕中，将网络映射到要使用的每个 ASA Virtual 接口。

网络可能没有按字母顺序排序。如果很难找到您的网络，可以稍后在“编辑设置”对话框中更改网络。在部署后，右键点击 ASA Virtual 实例，然后选择**编辑设置 (Edit Settings)** 以访问**编辑设置 (Edit Settings)** 对话框。但是，该屏幕不会显示 ASA Virtual 接口 ID（仅显示网络适配器 ID）。请参阅下面的网络适配器 ID 和 ASA Virtual 接口 ID 的索引：

网络适配器 ID	ASA Virtual 接口 ID
Network Adapter 1	Management 0/0
Network Adapter 2	GigabitEthernet 0/0
Network Adapter 3	GigabitEthernet 0/1
Network Adapter 4	GigabitEthernet 0/2
Network Adapter 5	GigabitEthernet 0/3
Network Adapter 6	GigabitEthernet 0/4
Network Adapter 7	GigabitEthernet 0/5
Network Adapter 8	GigabitEthernet 0/6
Network Adapter 9	GigabitEthernet 0/7
Network Adapter 10	GigabitEthernet 0/8

您不需要使用所有 ASA Virtual 接口；但是，vSphere Web 客户端要求为所有接口都分配网络。对于您不打算使用的接口，只需在 ASA Virtual 配置中禁用该接口。在部署 ASA Virtual 后，您可以返回到 vSphere Web 客户端以从“编辑设置”对话框中删除额外的接口。有关详细信息，请参阅 vSphere Web 客户端联机帮助。

注释
对于故障转移/HA 部署，GigabitEthernet 0/8 已预配置为故障转移接口。

步骤 7 如果网络使用 HTTP 代理来访问互联网，则必须在 **Smart Call Home 设置 (Smart Call Home Settings)** 区域中配置智能许可的代理地址。此代理一般也用于 Smart Call Home。

步骤 8 对于故障转移/HA 部署，请在“自定义模板”屏幕中进行如下配置：

- 指定备用管理 IP 地址。

  当您配置接口时，必须在相同网络上指定一个主用 IP 地址和一个备用 IP 地址。当主设备进行故障切换时，辅助设备会使用主设备的 IP 地址和 MAC 地址，并开始传送流量。此时处于备用状态的设备会接管备用 IP 地址和 MAC 地址。由于网络设备不会发现 MAC 与 IP 地址配对的变化，网络上的任意位置都不会发生 ARP 条目变化或超时。

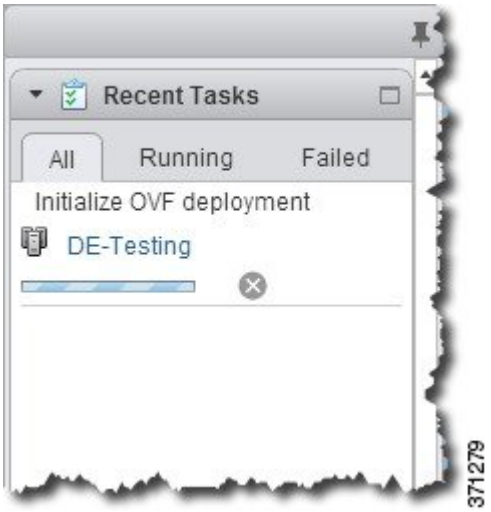
- 在 **HA Connection Settings** 区域中配置故障转移链路设置。

  故障转移对中的两台设备会不断地通过故障转移链路进行通信，以便确定每台设备的运行状态。GigabitEthernet 0/8 已预配置为故障转移链路。输入同一网络上的链路的活动和备用 IP 地址。

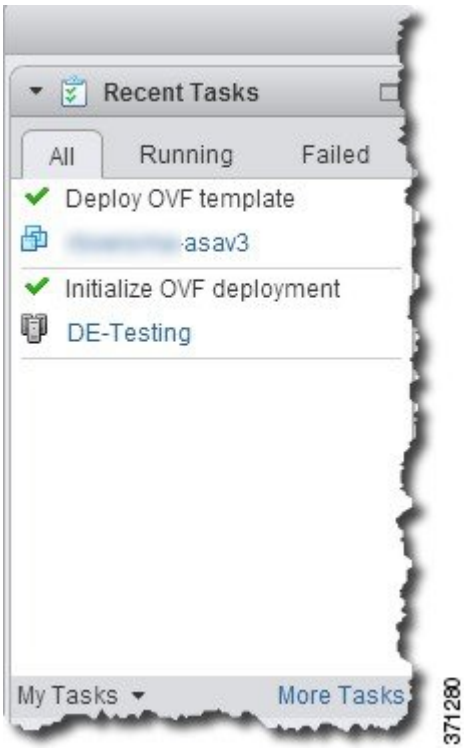
步骤 9 配置 OVF 参数**启用延迟监视程序计时器**以增加监视程序计时器阈值，以适应更长的磁盘 I/O 响应时间。

注释
此参数有助于防止在临时磁盘延迟峰值期间出现误报的监视程序触发和意外的 VM 重置。建议为对存储引起的停滞敏感或在可变 I/O 性能条件下运行的部署配置此参数。它特别用于使用网络存储（如 NFS）的环境中。

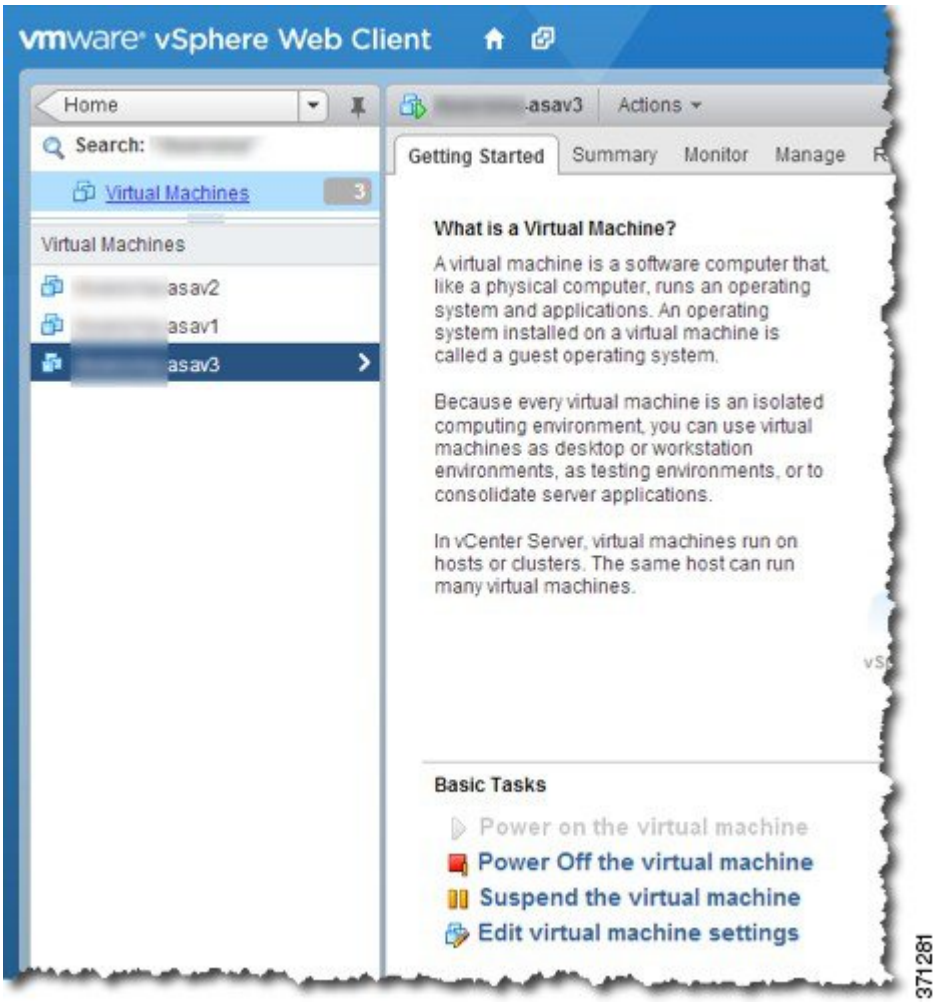
步骤 10 完成该向导后，vSphere Web 客户端将处理 VM；您可以在 **Global Information** 区域的 **Recent Tasks** 窗格中看到“初始化 OVF 部署”状态。



完成后，您会看到 Deploy OVF Template 完成状态。



随即在“清单”(Inventory) 中的指定数据中心下会显示 ASA Virtual机实例。



步骤 11 如果 ASA Virtual机尚未运行，请点击**启动虚拟机 (Power On the virtual machine)**。

等待 ASA Virtual 启动，然后尝试与 ASDM 或控制台连接。当 ASA Virtual 首次启动时，将读取通过 OVF 文件提供的参数，并将它们添加到 ASA Virtual 系统配置中。然后将自动重启引导过程，直到正常运行。仅当首次部署 ASA Virtual 时，才会出现双重启动过程。要查看启动消息，请点击**控制台 (Console)** 选项卡来访问 ASA Virtual 控制台。

步骤 12 对于故障转移/HA 部署，重复此过程以添加备用设备。请参阅以下准则：

- 设置与主设备相同的吞吐量级别。
- 输入与主设备完全相同的 *IP* 地址设置。除了用于标识设备是主设备还是备用设备的参数外，两个设备中的 bootstrap 配置相同。

下一步做什么

要向思科许可颁发机构成功注册 ASA Virtual，ASA Virtual需要访问互联网。部署之后，可能需要执行其他配置，以实现互联网访问和成功注册许可证。

使用 VMware vSphere 独立客户端和 Day 0 配置来部署 ASA Virtual

要部署 ASA Virtual，请使用 VMware vSphere 客户端和开放式虚拟化格式 (OVF) 模板文件（asav-vi.ovf 适用于 vCenter 部署，asav-esxi.ovf 适用于非 vCenter 部署）。在 vSphere 客户端中使用 Deploy OVF Template 向导来部署 ASA Virtual 的思科软件包。该向导将解析 ASA Virtual OVF 文件，创建将运行 ASA Virtual 的虚拟机，并安装软件包。

大多数向导步骤是 VMware 的标准步骤。有关 Deploy OVF Template 向导的更多信息，请参阅 VMware vSphere 客户端联机帮助。

开始之前

- 在部署 ASA Virtual 之前，您必须在 vSphere 中配置至少一个网络（用于管理）。
- 按照解压缩 ASA Virtual软件并创建 Day 0 配置文件，第 8 页中的步骤创建 Day 0 配置。

过程

步骤 1 启动 VMware vSphere 客户端，然后依次选择**文件 (File)** > **部署 OVF 模板 (Deploy OVF Template)**。

此时将出现“部署 OVF 模板”(Deploy OVF Template) 向导。

步骤 2 浏览至您将 asav-vi.ovf 文件解压缩到的工作目录，然后选择该文件。

步骤 3 此时将显示 OVF 模板详细信息。继续执行以下各个屏幕。如果您选择使用自定义 Day 0 配置文件，则不必更改任何配置。

步骤 4 最后一个屏幕会显示部署设置的摘要。点击**完成 (Finish)** 以部署虚拟机。

步骤 5 启动 ASA Virtual，打开 VMware 控制台，然后等待第二次启动。

步骤 6 通过 SSH 连接到 ASA Virtual 并完成所需的配置。如果 Day 0 配置文件中不具有您需要的所有配置，请打开 VMware 控制台并完成必要的配置。

ASA Virtual 现在完全正常运行。

使用 OVF 工具和 Day 0 配置来部署 ASA Virtual

本节介绍如何使用 OVF 工具部署 ASA Virtual，此部署需要 Day 0 配置文件。

开始之前

- 使用 OVF 工具部署 ASA Virtual时需要 day0.iso 文件。您可以使用默认的空 day0.iso 文件（压缩文件中提供），也可以使用您生成的自定义 Day 0 配置文件。要创建 Day 0 配置文件，请参阅解压缩 ASA Virtual软件并创建 Day 0 配置文件，第 8 页。
- 确保 OVF 工具已安装在 Linux 或 Windows PC 上，并且已连接到您的目标 ESXi 服务器。

过程

步骤 1 验证是否已安装 OVF 工具：

示例：

```
linuxprompt# which ovftool
```

步骤 2 使用所需的部署选项创建一个 .cmd 文件：

示例：

```
linuxprompt# cat launch.cmd
ovftool \
--name="asav-941-demo" \
--powerOn \
--deploymentOption=4Core8GB \
--diskMode=thin \
--datastore=datastore1 \
--acceptAllEulas \
--net:Management0-0="Portgroup_Mgmt" \
--net:GigabitEthernet0-1="Portgroup_Inside" \
--net:GigabitEthernet0-0="Portgroup_Outside" \
--prop:HARole=Standalone \
--prop:guestinfo.day0.iso=/home/user/day0.iso \
asav-esxi.ovf \
vi://root@10.1.2.3/
```

步骤 3 执行该 cmd 文件：

示例：

```
linuxprompt# ./launch.cmd
```

ASA Virtual启动；等待第二启动。

步骤 4 通过 SSH 连接到 ASA Virtual完成所需的配置。如果需要更多配置，请打开 VMware 控制台，进入 ASA Virtual，并应用必要的配置。

ASA Virtual 现在完全正常运行。

访问 ASA Virtual控制台

对于ASDM，在某些情况下可能需要使用CLI进行故障排除。默认情况下，您可以访问内置VMware vSphere 控制台，也可以配置网络串行控制台，它具有更好的功能，包括复制和粘贴。

- 使用 VMware vSphere 控制台
- 配置网络串行控制台端口

注释 如果使用 Day 0 配置文件部署 ASA Virtual, 可以在该配置文件中包括 **console serial** 设置，以便在首次启动过程中使用串行端口而不是虚拟 VGA 控制台；请参阅解压缩 ASA Virtual软件并创建 Day 0 配置文件，第 8 页。

使用 VMware vSphere 控制台

对于初始配置或故障排除，从通过 VMware vSphere Web 客户端提供的虚拟控制台访问 CLI。您可以稍后为 Telnet 或 SSH 配置 CLI 远程访问。

开始之前

对于 vSphere Web 客户端，安装客户端集成插件，该插件是访问 ASA Virtual控制台所必需的。

过程

步骤 1 在 VMware vSphere Web 客户端中，右键点击“清单”中的 ASA Virtual 实例，然后选择**打开控制台 (Open Console)**。或者，您可以点击“摘要”(Summary) 选项卡上的**启动控制台 (Launch Console)**。

步骤 2 点击控制台，然后按 **Enter** 键。注意：按 **Ctrl + Alt** 可释放光标。

如果 ASA Virtual 仍在启动，您会看到启动消息。

当 ASA Virtual 首次启动时，将读取通过 OVF 文件提供的参数，并将它们添加到 ASA Virtual 系统配置中。然后将自动重启引导过程，直到正常运行。仅当首次部署 ASA Virtual 时，才会出现双重启动过程。

注释
在安装许可证之前，吞吐量限制为 100 kbps，以便您可以执行初步连接测试。需要安装许可证才能正常运行。在安装许可证之前，您还会看到以下消息在控制台上重复出现：

```
Warning: ASAv platform license state is Unlicensed.
Install ASAv platform license for full functionality.
```

您将看到以下提示符：

```
ciscoasa>
```

此 提示符表明您正处于用户 EXEC 模式。用户 EXEC 模式仅能获取基本命令。

步骤 3 访问特权 EXEC 模式：

示例：

```
ciscoasa> enable
```

系统将显示以下提示：

```
Password:
```

步骤 4 按 **Enter** 键继续。默认情况下，密码为空。如果以前设置过启用密码，请输入该密码而不是按 Enter 键。

提示符更改为：

```
ciscoasa#
```

在特权 EXEC 模式中，所有非配置命令均可用。还可从特权 EXEC 模式进入 配置模式。

要退出特权模式，请输入 **disable**、**exit** 或 **quit** 命令。

步骤 5 访问全局配置模式：

```
ciscoasa# configure terminal
```

提示将更改为以下形式：

```
ciscoasa(config)#
```

可从全局配置模式开始配置 ASA Virtual。要退出全局配置模式，请输入 **exit**、**quit** 或 **end** 命令。

配置网络串行控制台端口

为获得更好的控制台体验，可以单独配置网络串行端口或连接到虚拟串行端口集中器 (vSPC) 进行控制台访问。有关每种方法的详细信息，请参阅 VMware vSphere 文档。在 ASA Virtual 上，您必须将控制台输出发送到串行端口而不是虚拟控制台。此程序介绍如何启用串行端口控制台。

过程

步骤 1 在 VMware vSphere 中配置网络串行端口。请参阅 VMware vSphere 文档。

步骤 2 在 ASA Virtual 上的 disk0 的根目录下创建一个名为“use_ttyS0”的文件。此文件不需要有任何内容；它只需在以下位置存在：

disk0:/use_ttyS0

- 在 ASDM 中，可以使用**工具 (Tools)** > **文件管理 (File Management)**对话框上传该名称的空文本文件。
- 在 vSphere 控制台中，您可以将文件系统中的现有文件（任何文件）复制为新名称。例如：

```
ciscoasa(config)# cd coredumpinfo
ciscoasa(config)# copy coredump.cfg disk0:/use_ttyS0
```

步骤 3 重新加载 ASA Virtual。

- 在 ASDM 中依次选择**工具 (Tools)** > **系统重新加载 (System Reload)**。

- 在 vSphere 控制台中，输入 **reload**。

  ASA Virtual 停止发送到 vSphere 控制台，而是发送到串行控制台。

步骤 4 Telnet 到您在添加串行端口时指定的 vSphere 主机 IP 地址和端口号，或 Telnet 到 vSPC IP 地址和端口。

升级 vCPU 或吞吐量许可证

ASA Virtual 使用吞吐量许可证，它会影响您可以使用的 vCPU 数量。

如果要增加（或减少）ASA Virtual 的 vCPU 数量，您可以申请新许可证，应用新许可证，并在 VMware 中更改 VM 属性以匹配新值。

注释 分配的 vCPU 数量必须与 ASA Virtual CPU 许可证或吞吐量许可证相符。RAM 也必须针对 vCPU 数量进行正确调整。升级或降级时，请务必按照此过程操作并立即调整许可证和 vCPU。如果存在持续不匹配，ASA Virtual 无法正常工作。

过程

步骤 1 申请新许可证。

步骤 2 应用新许可证。对于故障转移对，将新许可证应用到两个设备。

步骤 3 执行以下操作之一，具体取决于是否使用故障转移：

- 有故障转移 - 在 vSphere Web 客户端中，关闭备用 ASA Virtual。例如，点击 ASA Virtual，然后点击**关闭虚拟机 (Power Off the virtual machine)**，或者右键点击 ASA Virtual，然后选择**关闭访客操作系统 (Shut Down Guest OS)**。
- 无故障转移 - 在 vSphere Web 客户端中，关闭 ASA Virtual。例如，点击 ASA Virtual，然后点击**关闭虚拟机 (Power Off the virtual machine)**，或者右键点击 ASA Virtual，然后选择**关闭访客操作系统 (Shut Down Guest OS)**。

步骤 4 点击 ASA Virtual，然后点击**编辑虚拟机设置 (Edit Virtual machine settings)**（或者右键点击 ASA Virtual，然后选择**编辑设置 (Edit Settings)**）。

系统将显示**编辑设置 (Edit Settings)** 对话框。

步骤 5 请参阅许可 ASA Virtual中的 CPU/内存要求以确定新 vCPU 许可证的正确值。

步骤 6 在**虚拟硬件 (Virtual Hardware)** 选项卡上，从下拉列表中为 **CPU** 选择新值。

步骤 7 对于 **Memory**，输入 RAM 的新值。

步骤 8 点击**确定 (OK)**。

步骤 9 打开 ASA Virtual 的电源。例如，点击**启动虚拟机 (Power On the Virtual Machine)**。

步骤 10 对于故障转移对：

1. 打开主用设备的控制台或启动主用设备上的 ASDM。
2. 备用设备完成启动后，故障切换到备用设备：
   - ASDM：依次选择**监控 (Monitoring)** > **属性 (Properties)** > **故障转移 (Failover)** > **状态 (Status)**，然后点击**设为备用 (Make Standby)**。
   - CLI： **failover active**
3. 对活动设备重复步骤 3 到 9。

下一步做什么

有关详细信息，请参阅许可 ASA Virtual。

性能调优

提高 ESXi 配置的性能

通过调整 ESXi 主机的 CPU 配置设置，可以提高 ESXi 环境中的 ASA Virtual 性能。通过调度关联选项，可以控制虚拟机 CPU 在主机物理核心（和超线程，如果已启用超线程）范围内的分布方式。使用此功能，您可以将每个虚拟机分配到指定关联组中的处理器。

有关详细信息，请参阅以下 VMware 文档。

- 《vSphere 资源管理》的 *CPU* 资源管理一章。
- 《VMware vSphere 的性能最佳实践》。
- vSphere 客户端联机帮助。

NUMA 准则

非一致内存访问 (NUMA) 是一种共享内存架构，描述了多处理器系统中主内存模块相对于处理器的位置。如果处理器访问的内存不在自己的节点内（远程内存），则数据通过 NUMA 连接以低于本地内存的访问速率传输。

X86 服务器架构由多个插槽和每个插槽内的多个内核组成。每个 CPU 插槽及其内存和 I/O 均称为 NUMA 节点。要从内存高效读取数据包，来宾应用和关联的外围设备（例如 NIC）应位于同一个节点中。

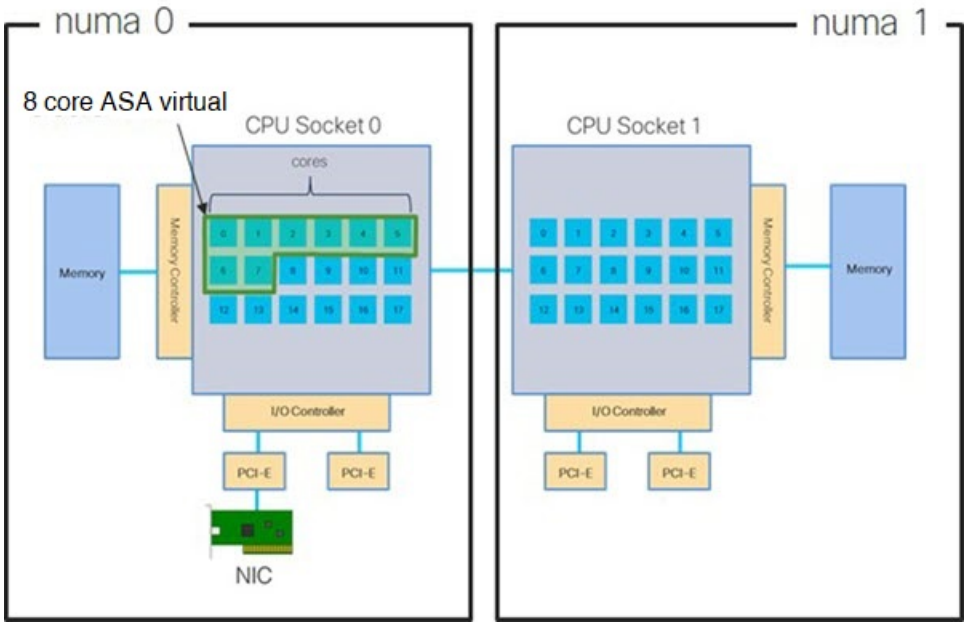
为获得最佳 ASA Virtual性能：

- ASA Virtual VM 必须在单一 NUMA 节点上运行。如果部署了单个 ASA Virtual以跨 2 个插槽运行，则性能将显著下降。
- 8 核 ASA Virtual (图 1: 8 核 NUMA 架构示例，第 23 页) 要求主机 CPU 上的每个插槽至少有 8 个内核。必须考虑服务器上运行的其他虚拟机。
- 16 核 ASA Virtual (图 2: 16 核 ASA Virtual NUMA 架构示例，第 24 页) 要求主机 CPU 上的每个插槽至少有 16 个内核。必须考虑服务器上运行的其他虚拟机。
- NIC 应与 ASA Virtual机位于同一 NUMA 节点上。

注释 ASA Virtual 不支持物理核心的多非一致内存访问 (NUMA) 节点和多个 CPU 插槽。

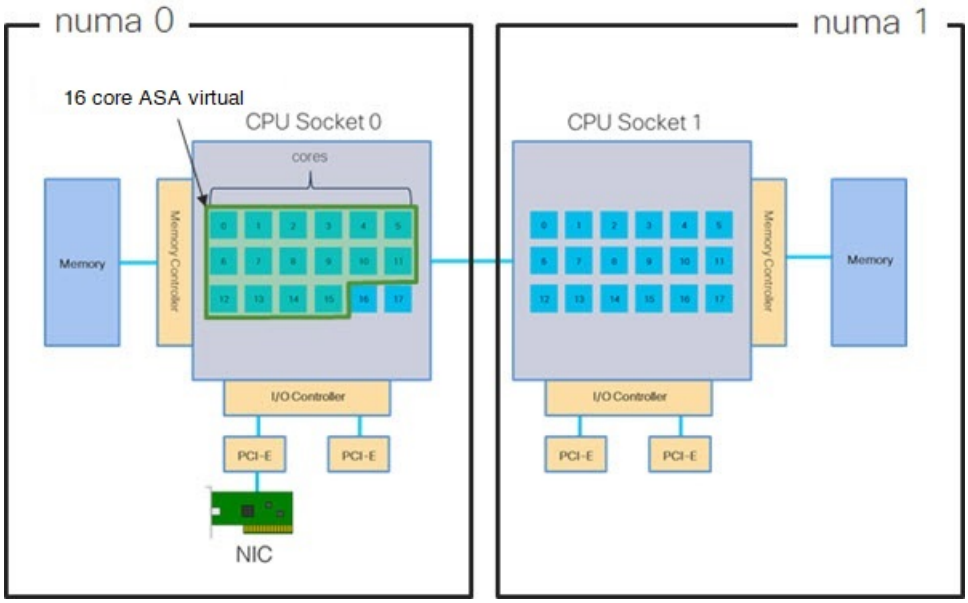
下图显示的服务器有两个 CPU 插槽，每个 CPU 有 18 个内核。8 核 ASA Virtual要求主机 CPU 上的每个插槽至少有 8 个内核。

图 *1: 8* 核 *NUMA* 架构示例



下图显示的服务器有两个 CPU 插槽，每个 CPU 有 18 个内核。16 核 ASA Virtual要求主机 CPU 上的每个插槽至少有 16 个内核。

图 *2: 16* 核 *ASA Virtual NUMA* 架构示例



有关在 ESXi 上使用 NUMA 系统的详细信息，请参阅您的 VMware ESXi 版本对应的 VMware 文档 *vSphere* 资源管理。要查看此文档和其他相关文档的最新版本，请参阅 http://www.vmware.com/support/pubs

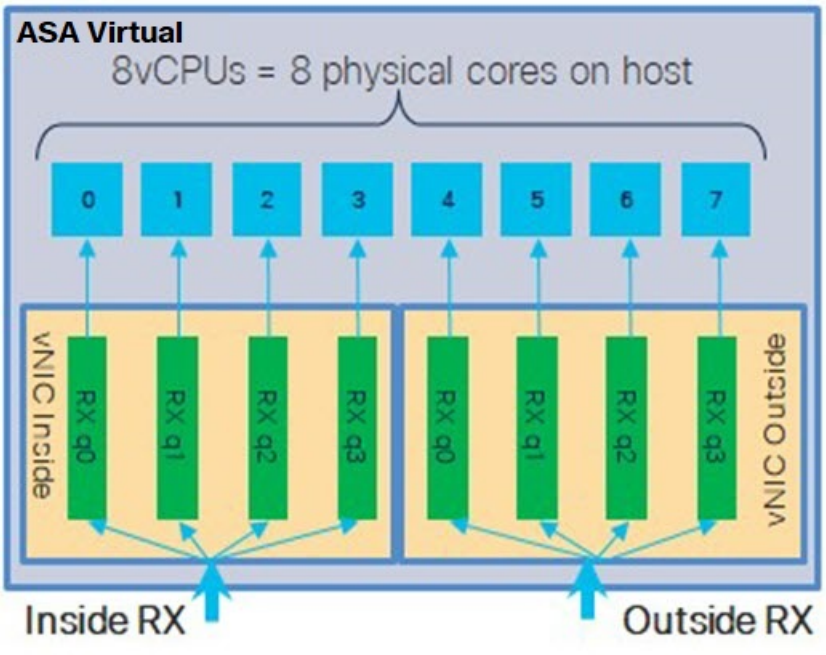
用于接收端扩展 (RSS) 的多个 RX 队列

ASA Virtual支持接收端扩展 (RSS)，网络适配器利用这项技术将网络接收流量并行分发给多个处理器内核。为实现最大吞吐量，每个 vCPU（内核）都必须有自己的 NIC RX 队列。请注意，典型的 RA VPN 部署可能使用单一内部/外部接口对。

重要事项 您需要 ASA Virtual版本 9.13(1) 或更高版本，才能使用多个 RX 队列。

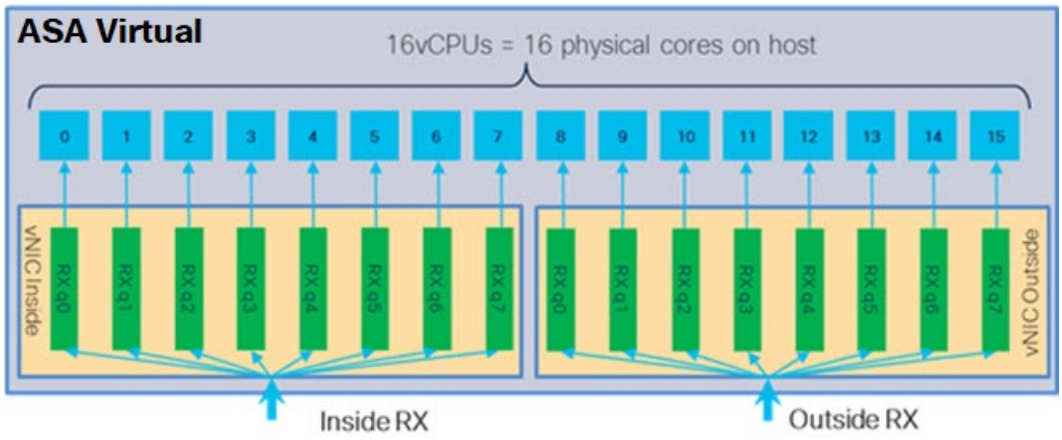
对于具有内部/外部接口对的 8 核 VM，每个接口将有 4 个 RX 队列，如图 3: 8 核 ASA Virtual RSS RX 队列，第 25 页中所示。

图 *3: 8* 核 ***ASA Virtual RSS RX*** 队列



对于具有内部/外部接口对的 16 核 VM，每个接口将有 8 个 RX 队列，如图 4: 16 核 ASA Virtual RSS RX 队列，第 25 页中所示。

图 *4: 16* 核 ***ASA Virtual RSS RX*** 队列



下表显示了适用于 VMware 的 ASA Virtual vNIC 以及支持的 RX 队列数量。有关支持的 vNIC 的说明，请参阅建议的 vNIC，第 2 页。

表 *3: VMware* 建议的 *NIC/vNIC*

NIC 卡	vNIC 驱动程序	驱动程序技术	RX 队列数	性能
x710*	i40e	PCI 直通	最多 8 个	PCI 直通为测试的 NIC 提供最高性能。在直通模式下，NIC 专用于 ASA Virtual，不是最佳虚拟选项。
	i40evf	SR-IOV	4	具有 x710 NIC 的 SR-IOV 吞吐量低于（约 30%）PCI 直通。VMware 上每个 i40evf 最多有 4 个 RX 队列。16 核 VM 要达到最大吞吐量，需要 8 个 RX 队列。
x520	ixgbe-vf	SR-IOV	2	-
	ixgbe	PCI 直通	6	ixgbe 驱动程序（在 PCI 直通模式下）有 6 个 RX 队列。性能与 i40evf (SR-IOV) 不相上下。
不适用	vmxnet3	并行虚拟化	最多 8 个	不建议用于 ASAv100。
不适用	e1000	不建议使用 VMware。		
*ASA Virtual 与 x710 NIC 的 1.9.5 i40en 主机驱动程序不兼容。较旧或更新版本的驱动程序将正常工作。有关识别或验证 NIC 驱动程序和固件版本的 ESXCLI 命令的信息，请参阅识别 NIC 驱动程序和固件版本，第 26 页。				

识别 NIC 驱动程序和固件版本

如果您需要识别或验证特定的固件和驱动程序版本信息，可以使用 ESXCLI 命令查找该数据。

- 要获取已安装 NIC 的列表，通过 SSH 连接相关主机，然后运行 `esxcli network nic list` 命令。此命令应为您提供设备和一般信息的记录。
- 在得到已安装 NIC 的列表后，您可以提取详细的配置信息。运行 `esxcli network nic get` 命令指定必要的 NIC 名称：`esxcli network nic get -n <nic name>`。

注释 一般网络适配器信息也可以从 VMware vSphere Client 查看。在**配置 (Configure)** 选项卡中的**物理适配器 (Physical Adapters)** 下可找到适配器和驱动程序。

SR-IOV 接口调配

SR-IOV 允许多个 VM 共享主机内的单一 PCIe 网络适配器。SR-IOV 定义了下列功能：

- 物理功能 (PF) - PF 指所有 PCIe 功能，包括 SR-IOV 功能。这些功能在主机服务器上显示为常规静态 NIC。
- 虚拟功能 (VF) - VF 是有助于数据传输的轻型 PCIe 功能。VF 源自于 PF，并通过 PF 进行管理。

VF 在虚拟化操作系统框架下，最高可以 10 Gbps 的速度连接 ASA Virtual机。本节介绍如何在 KVM 环境下配置 VF。ASA Virtual和 SR-IOV 接口调配中介绍了 ASA Virtual上对 SR-IOV 的支持信息。

在 ASAv5 和 ASAv10 上，强烈建议使用 VMXNET3 驱动程序以实现最佳性能。此外，SR-IOV 接口与 ASA Virtual组合使用时（混合接口），尤其是在分配更多 CPU 核心和资源时。

准则和限制

SR-IOV 接口准则

VMware vSphere 5.1 及更高版本仅在具有特定配置的环境下支持 SR-IOV。启用 SR-IOV 时，vSphere 的某些功能无法正常工作。

除了SR-IOV 接口准则和限制中所述的 ASA Virtual和 SR-IOV 的系统要求之外，您还应该查看 VMware 文档中的支持使用 SR-IOV 的配置，以了解有关要求、支持的 NIC、功能可用性及 VMware 和 SR-IOV 升级要求方面的详细信息。

VMware 上使用 SR-IOV 接口的 ASA Virtual 支持混合接口类型。您可以将 SR-IOV 或 VMXNET3 用于管理接口，并将 SR-IOV 用于数据接口。

本节介绍在 VMware 系统上调配 SR-IOV 接口的各种设置和配置步骤。本节中的信息基于特定实验室环境中的设备创建，这些设备使用的是 VMware ESXi 6.0 和 vSphere Web 客户端、思科 UCS C 系列服务器及 Intel 以太网服务器适配器 X520 - DA2。

SR-IOV 接口的限制

启动 ASA Virtual 时，请注意 SR-IOV 接口出现的顺序可能与 ESXi 中显示的顺序相反。这可能引起接口配置错误，导致特定的 ASA Virtual机无网络连接。

⚠

注意 开始在 ASA Virtual 上配置 SR-IOV 网络接口之前，先验证接口映射非常重要。这可确保将网络接口配置应用到 VM 主机上正确的物理 MAC 地址接口。

ASA Virtual 启动后，您可以确认哪个 MAC 地址映射到哪个接口。请使用 **show interface** 命令查看详细的接口信息，包括接口的 MAC 地址。将 MAC 地址与 **show kernel ifconfig** 命令的结果进行比较以确认正确的接口分配。

检查 ESXi 主机 BIOS

要在 VMware 上部署带 SR-IOV 接口的 ASA Virtual，需要支持和启用虚拟化。VMware 提供了几种验证虚拟化支持的方法，包括其在线 SR-IOV 支持兼容性指南以及可下载的 CPU 识别实用程序（检测虚拟化处于启用还是禁用状态）。

另外，您还可以通过登录到 ESXi 主机来确定是否在 BIOS 中启用了虚拟化。

过程

步骤 1 使用下列方法之一登录到 ESXi Shell：

- 如果您可以直接访问主机，请按 Alt+F2 打开计算机物理控制台的登录页面。
- 如果您正在远程连接主机，请使用 SSH 或其他远程控制台连接在主机上启动会话。

步骤 2 输入主机识别的用户名和密码。

步骤 3 运行以下命令：

示例：

```
esxcfg-info|grep "\----\HV Support"
```

HV Support 命令的输出指示可用的虚拟机监控程序类型。有关可能值的说明如下：

0 - VT/AMD-V 表示该支持对于此硬件不可用。

1 - VT/AMD-V 表示 VT 或 AMD-V 可能可用，但此硬件不支持它们。

2 - VT/AMD-V 表示 VT 或 AMD-V 可用，但目前在 BIOS 中未启用。

3 - VT/AMD-V 表示 VT 或 AMD-V 在 BIOS 中已启用，并且可以使用。

示例：

```
~ # esxcfg-info|grep "\----\HV Support"
         |----HV Support.........................3
```

值 3 表示受支持且已启用虚拟化。

下一步做什么

- 在主机物理适配器上启用 SR-IOV。

在主机物理适配器上启用 SR-IOV

使用 vSphere Web 客户端启用 SR-IOV，并设置主机上的虚拟功能数量。在执行此操作之前，您无法将虚拟机连接到虚拟功能。

开始之前

- 请确保已安装兼容 SR-IOV 的网络接口卡 (NIC)；请参阅SR-IOV 支持的 NIC。

过程

步骤 1 在 vSphere Web 客户端中，导航到要启用 SR-IOV 的 ESXi 主机。

步骤 2 在**管理 (Manage)** 选项卡上，点击**网络 (Networking)** 并选择**物理适配器 (Physical adapters)**。

您可以查看 SR-IOV 属性，以了解物理适配器是否支持 SR-IOV。

步骤 3 选择物理适配器，然后点击**编辑适配器设置 (Edit adapter settings)**。

步骤 4 在 SR-IOV 下，从**状态 (Status)** 下拉菜单中选择**启用 (Enabled)**。

步骤 5 在**虚拟功能数量 (Number of virtual functions)** 文本框中，键入要为该适配器配置的虚拟功能数目。

注释
对于 ASAv50，我们建议您对每个接口使用的 VF 数量**不要**超过 1 个。如果与多个虚拟功能共享物理接口，可能会出现性能下降。

步骤 6 点击**确定 (OK)**。

步骤 7 重启 ESXi 主机。

虚拟功能在由物理适配器项表示的 NIC 端口上将变为活动状态。它们显示在主机**设置 (Settings)**选项卡的“PCI 设备”(PCI Devices) 列表中。

下一步做什么

- 创建一个标准 vSwitch 来管理 SR-IOV 功能和配置。

创建 vSphere 交换机

创建一个 vSphere 交换机来管理 SR-IOV 接口。

过程

步骤 1 在 vSphere Web 客户端中，导航至 ESXi 主机。

步骤 2 在**管理 (Manage)** 下，选择**网络 (Networking)**，然后选择**虚拟交换机 (Virtual switches)**。

步骤 3 点击**添加主机网络 (Add host networking)**图标，即带有加号 (+) 的绿色地球仪图标。

步骤 4 选择**标准交换机的虚拟机端口组 (Virtual Machine Port Group for a Standard Switch)** 连接类型，然后点击**下一步 (Next)**。

步骤 5 选择**新建标准交换机 (New standard switch)**，然后点击**下一步 (Next)**。

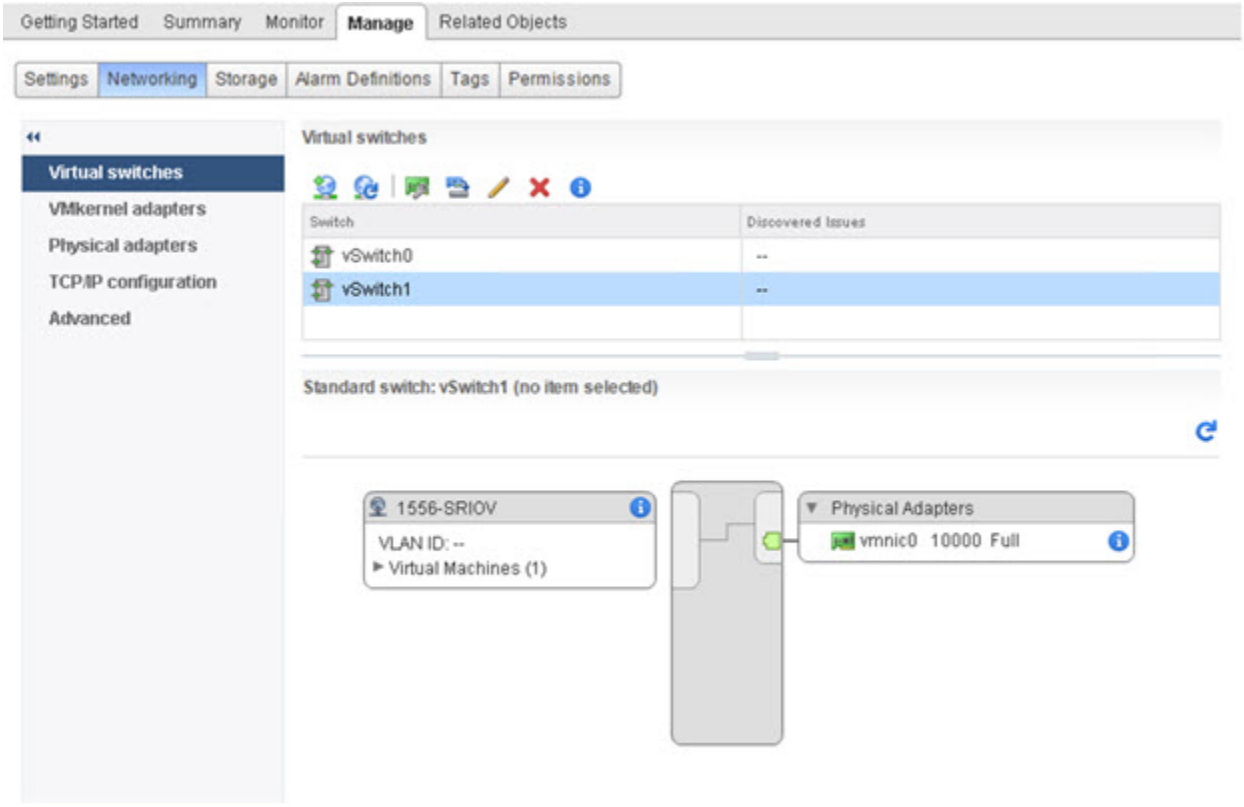
步骤 6 将物理网络适配器添加到新的标准交换机中。

a) 在分配的适配器下，点击绿色加号 (+) 以**添加适配器**。
b) 从列表中为 SR-IOV 选择相应的网络接口。例如 Intel(R) 82599 万兆位双端口网络连接。
c) 从**故障转移顺序组 (Failover order group)**下拉菜单中，选择**活动适配器 (Active adapters)**。
d) 点击**确定 (OK)**。

步骤 7 为该 SR-IOV vSwitch 输入一个**网络标签**，然后点击**下一步 (Next)**。

步骤 8 在**准备完成 (Ready to complete)** 页面上查看您的选择，然后点击**完成 (Finish)**。

图 *5:* 已连接 ***SR-IOV*** 接口的新 ***vSwitch***



下一步做什么

- 查看虚拟机的兼容级别。

升级虚拟机的兼容级别

兼容级别决定可用于虚拟机的虚拟硬件，它们与主机上可用的物理硬件相对应。ASA Virtual虚拟机的硬件级别需要达到 10 级或更高级别。这样才能将 SR-IOV 直通功能暴露给 ASA Virtual。以下操作程序可立即将 ASA Virtual 升级到最新支持的虚拟硬件版本。

有关虚拟机硬件版本和兼容性的信息，请参阅 vSphere 虚拟机管理文档。

过程

步骤 1 从 vSphere Web 客户端登录到 vCenter 服务器。

步骤 2 找到要修改的 ASA Virtual计算机。

a) 选择数据中心、文件夹、集群、资源池或主机，然后点击**相关对象 (Related Objects)** 选项卡。

b) 点击**虚拟机 (Virtual Machines)**，并从列表中选择 ASA Virtual机。

步骤 3 关闭所选的虚拟机。

步骤 4 右键点击该 ASA Virtual，并依次选择**操作 (Actions)** > **所有 vCenter 操作 (All vCenter Actions)** > **兼容性 (Compatibility)** > **升级 VM 兼容性 (Upgrade VM Compatibility)**。

步骤 5 点击**是 (Yes)** 以确认升级。

步骤 6 为虚拟机兼容性选择 **ESXi 5.5 及更高版本 (ESXi 5.5 and later)**选项。

步骤 7 （可选）选择**仅在正常访客操作系统关闭后升级 (Only upgrade after normal guest OS shutdown)**。

所选虚拟机将升级为您选择的相应硬件版本的兼容性设置，并且虚拟机的摘要选项卡中将更新为新的硬件版本。

下一步做什么

- 通过 SR-IOV 直通网络适配器将该 ASA Virtual 与虚拟功能关联。

将 SR-IOV NIC 分配给 ASA Virtual

为了确保 ASA Virtual机和物理 NIC 可以交换数据，您必须将 ASA Virtual 与一个或多个用作 SR-IOV 直通网络适配器的虚拟功能相关联。以下操作程序说明如何使用 vSphere Web 客户端将 SR-IOV NIC 分配给 ASA Virtual机。

过程

步骤 1 从 vSphere Web 客户端登录到 vCenter 服务器。

步骤 2 找到要修改的 ASA Virtual计算机。

a) 选择数据中心、文件夹、集群、资源池或主机，然后点击**相关对象 (Related Objects)** 选项卡。

b) 点击**虚拟机 (Virtual Machines)**，并从列表中选择 ASA Virtual机。

步骤 3 在虚拟机的**管理 (Manage)**选项卡上，依次选择**设置 (Settings)** > **VM 硬件 (VM Hardware)**。

步骤 4 点击**编辑 (Edit)**，然后选择**虚拟硬件 (Virtual Hardware)** 选项卡。

步骤 5 从**新建设备 (New device)** 下拉菜单中，选择**网络 (Network)**，然后点击**添加 (Add)**。

系统将显示**新建网络 (New Network)** 界面。

步骤 6 展开**新建网络 (New Network)** 部分，然后选择可用的 SRIOV 选项。

步骤 7 从**适配器类型 (Adapter Type)**下拉菜单中选择 **SR-IOV 直通 (SR-IOV passthrough)**。

步骤 8 从**物理功能 (Physical function)** 下拉菜单中，选择与直通虚拟机适配器相对应的物理适配器。

步骤 9 接通虚拟机电源。

接通虚拟机电源后，ESXi 主机将从物理适配器中选择一个可用的虚拟功能，并将其映射到 SR-IOV 直通适配器。主机将验证虚拟机适配器和底层虚拟功能的所有属性。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。